IN THE SPECIFICATION:

On page 16, please amend the paragraph beginning at line 6 as follows:

--Now, assume that the memory circuit 130 of the device for some reason looses its content. This implies that all cryptographic keys that were stored in the device during assembly will be lost. Via a third party application server which ~~interact~~interacts with the public database 170 over, e.g. the Internet, the owner of the personal device will then be able to restore some of the lost data in the flash memory without any interaction with a service point and/or a secret database.--

On page 16, please amend the paragraph beginning at line 15 as follows:

--The recovery of the essential flash memory data is achieved by first reading the unique chip identifier from the read-only storage 120 of the personal device 100. The chip identifier is then sent to an on-line system incorporating the public database 170. The on-line system returns the corresponding backup data package and certificate for the unique device identity, without having to access any secret information. The owner is then able to create a new flash image using the received copy of the backup data package and the certificate. When the device 100 then is booted up, the device will recognize the backup code attached to the received backup data package and start to decrypt the backup data package to a data package which is identical to the data package originally stored in the flash memory during assembly of the device by the manufacturer. Moreover, the recovery of the flash content also includes recovery of the unique device identity that has been allocated to the device. It should not be possible for anyone to change this device identity during a recovery, but ~~is~~it should be the same as that originally stored by the manufacturer. To ensure this, the device uses the manufacturer's public signature key stored in the ROM memory of the device to verify the certificate and verify the authenticity of the device identity. This operation is thus performed without any interaction from the manufacturer. If this verification is successful, the cryptographic keys and the unique device identity, and possibly some other data, which were associated with device during its assembly by the manufacturer, will be fully restored in the memory circuit 130.--